AMENDMENTS TO THE CLAIMS

1. (Currently Amended) A method of activating a smart card, comprising:

receiving identifying information for a non-activated smart card that is being used for the first time by a user;

receiving manual authentication information for the user to whom the non-activated smart card has been issued;

authenticating the user and the non-activated smart card using the identifying information and the manual authentication information;

obtaining a public key from the non-activated smart card; and

issuing a digital certificate that is generated using the public key, wherein the non-activated smart cart is activated upon receiving the digital certificate.

2. (Previously Amended) The method according to claim 1, wherein the manual authentication information comprises a user identifier and a password.

3. (Original) The method according to claim 1, further comprising obtaining the digital certificate from a certificate authority.

4. (Previously Amended) The method according to claim 1, wherein the smart card is connected to a workstation.

5. (Previously Amended) The method according to claim 1, wherein the digital certificate is stored in at least one of the activated smart

card and a workstation.

6. (Previously Amended) The method according to claim 1, further comprising:

receiving a login request that is initiated when the activated smart card is connected to a workstation;

authenticating the activated smart card using the digital certificate; and

if authenticated, permitting a login to a computer resource.

7. (Previously Amended) The method according to claim 6, wherein the activated smart card is removed from the workstation after it is authenticated.

8. (Previously Amended) The method according to claim 6, wherein authenticating the activated smart card further comprises determining that the digital certificate has not been revoked.

9. (Currently Amended) A method of activating a smart card, comprising:

sending, to an administration server, identifying information read from a non-activated smart card that has not been previously used by a user to whom the non-activated smart card has been issued;

sending, to the administration server, manual authentication information input by ~~a~~ the user ~~to whom the non-activated smart card has been issued~~;

generating a public key using the non-activated smart card;

sending the public key to the administration server; and

receiving a digital certificate that is generated using the public key, wherein the non-activated smart card is activated upon receipt of the digital certificate.

10. (Previously Amended) The method according to claim 9, wherein the manual authentication information comprises a user identifier and a password.

11. (Original) The method according to claim 9, further comprising receiving the digital certificate from a certificate authority.

12. (Previously Amended) The method according to claim 9, wherein the smart card is connected to a workstation.

13. (Previously Amended) The method according to claim 9, further comprising storing the digital certificate in at least one of the activated smart card and a workstation.

14. (Previously Amended) The method according to claim 9, further comprising:

connecting the activated smart card to a workstation;

sending a login request to a server that authenticates the digital certificate against a certificate revocation list; and

if authenticated, permitting a login to a computer resource.

15. (Previously Amended) The method according to claim 14, wherein the activated smart card is removed from the workstation after the digital certificate is sent.

16. (Previously Amended) The method according to claim 14, wherein the server determines that the digital certificate has not been revoked.

Claims 17-22 (Canceled).

23. (Currently Amended) A method of activating a smart card then using ~~a~~ an activated smart card, comprising:

on first use of ~~the~~ a non-activated smart card by a user to whom the non-activated smart card has been issued:

receiving identifying information for ~~a~~ the non-activated smart card;

receiving manual identification information for ~~a~~ the user ~~to whom the non-activated smart card has been issued~~;

authenticating the user and the non-activated smart card using the manual authentication information and the identifying information;

obtaining a public key from the non-activated smart card; and

sending a digital certificate generated using the public key from a certificate authority to the non-activated smart card, wherein the non-activated smart card is activated upon receiving the digital

certificate; and

on a subsequent use of the smart card:

receiving a login request that is initiated when the activated smart card is connected to a workstation;

authenticating the digital certificate against a certificate revocation list to determine that the digital certificate has not been revoked; and

if authenticated, permitting a login to a computer resource.

24. (Previously Amended) The method according to claim 23, wherein the activated smart card is connected to a workstation and removed from the workstation after it is authenticated.

25. (Previously Amended) The method according to claim 23, wherein the digital certificate is stored in at least one of the activated smart card and a workstation.

AMENDMENTS TO THE SPECIFICATION

The paragraph on page 2, lines 11-22, is amended as follows:

In one embodiment of the present invention a simplified user authentication to a computer resource is provided utilizing a smart card. When a new user is issued a smart card, he or she is also issued a user name (ID) and password to be used during a first use to activate the smart card. The user then connects the smart card and enters the user ID and password. The user is authenticated using the user ID and password and identifying information from the smart card. The network administration server then requests a public key from the workstation. The workstation instructs the smart card to ~~generates~~ generate public and private ~~key~~ keys. The public key is transmitted to the server. A digital certificate is created and the smart card is activated. Once the smart card is activated a simplified login procedure can be used wherein connecting the smart card to a workstation initiates a login process not requiring use of a PIN number or other user input.

The paragraph beginning at page 5, line 24, and continuing to page 6, line 11, is amended as follows:

Turning now to FIGURE 1, an exemplary network 100 is illustrated. A smart card 110 can be inserted into an appropriate connector in a smart card reader 114. Smart card reader 114 is connected to, or forms apart of, a workstation 120 connected to a computer network 126. Access to the network resources and issuance of smart cards, passwords, login

identification, etc. is administered using an administration server 130 which is coupled to network information services or directory services (NIS/DS) database 134. In network 100, administration server 130 also provides the function of administration of digital certificates. Smart card 110 is utilized by a user to obtain access to any of the computing resources available in network 126 including various file servers and the like. Depending upon the level of security required, it may be desirable to permit a user to login using smart card 110 as the only authentication mechanism. That is, while conventional security systems require a smart card 110 in combination with personal identification number PIN, in less secure situations it may be useful to permit connection of the smart card 110 to initiate a user login. Moreover, it may also be desirable to permit a user to activate a smart card 110 without intensive involvement of network administration ~~personal~~ personnel.

The paragraph on page 8, lines 11-27, is amended as follows:

Process 230 of FIGURE 6 describes use of a smart card 110 as an aide to simplified login and to provide authentication starting at 604. At 610, the process determines if the smart card 110 is connected, and if not, awaits connection of a smart card 110. Once a smart card 110 is connected to the workstation 120 at 610, the smart card 110, in conjunction with the workstation 120, initiates a login at 616. This may be accomplished, for example, by sending a message out over the network alerting network servers that a smart card 110 is connected. The smart card 110 is then authenticated at 620. This may be accomplished, for example, by

challenging the smart card 110 to carry out ~~and~~ an encryption operation using its private key. If the encrypted information can be correctly decrypted at the server using the public key, then it is presumed ~~to~~ that the smart card 110 is properly authenticated. The authentication process of 620 also utilizes the digital certificate and verifies that the certificate has not been revoked at 640 as a further portion of the authentication process. If the certificate is not good (for example if the certificate is indicated as having been revoked by its presence on a certificate revocation list) the login is rejected at 654. If the certificate is good at 648, login is authorized at 660 and process ends at 668.

REMARKS

Claims 1-16 and 23-25 are pending. Claims 1, 9 and 23 are amended herein.

Response to Examiner's Comments

In the Advisory Action mailed September 9, 2003, the Examiner states that the prior art of record (Muftic) still meets the limitations of the claimed invention. Applicants respectfully disagree. While Muftic suggests that non-activated smart cards should be personalized, Muftic does not show or suggest a method of doing so. There can be different ways of activating a smart card. The instant application describes at least a conventional approach and a claimed approach. Because Muftic lacks the specifics of an approach for personalizing a smart card, Applicants respectfully submit that Muftic does not read on the present claimed invention. Further discussion of this point is provided in the remarks below.

102 Rejections

Claims 1-6 and 9-13 are rejected under 35 U.S.C. § 102(b) as being anticipated by Muftic (US 5,943,423). The Applicants have reviewed the cited reference and respectfully assert that Muftic does not show or suggest the embodiments of the present invention recited in Claims 1-6 and 9-13.

Claims 1 and 9 are amended herein to more clearly describe the present claimed invention. More specifically, embodiments of the present invention pertain to methods of activating a non-activated smart card. As

recited in the amended claims, a non-activated smart card refers to a new card that has not been previously used by a particular user. Once the smart card is activated, the user can then gain access to computing resources, for example.

Given the context of the claims as described above, the Applicants respectfully submit that Muftic does not show or suggest activating a non-activated smart card. Reference is made to column 10, lines 58-62, of Muftic, which states "When received from the manufacturer, smart cards are essentially blank. They must be formatted, for example, to effectuate the data architecture shown in FIG. 4 and they must be personalized with information for the specific user to which the card will be assigned" (emphasis added).

However, Muftic does not show or suggest a method for personalizing a smart card. In other words, bearing in mind the manner in which "non-activated" and "activating" are used in the claims, Applicants respectfully submit that Muftic does not show or suggest methods for activating a non-activated smart card. While Muftic suggests that non-activated smart cards should be personalized, Muftic does not show or suggest a method of doing so. As described in the instant application, there can be different ways of activating a smart card. The instant application describes at least a conventional approach and a claimed approach. Because Muftic lacks a description of an approach for personalizing a smart card, Muftic does not read on the present claimed invention.

Specifically, Applicants respectfully submit that Muftic does not show or suggest "receiving identifying information for a non-activated smart card that is being used for the first time by a user; receiving manual authentication information for the user to whom the non-activated smart card has been issued; authenticating the user and the non-activated smart card using the identifying information and the manual authentication information; obtaining a public key from the non-activated smart card; and issuing a digital certificate that is generated using the public key, wherein the non-activated smart cart is activated upon receiving the digital certificate" as recited in independent Claim 1. Claims 2-6 are dependent on Claim 1.

Furthermore, Applicants respectfully submit that Muftic does not show or suggest "sending, to an administration server, identifying information read from a non-activated smart card that has not been previously used by a user to whom the non-activated smart card has been issued; sending, to the administration server, manual authentication information input by ~~a~~ the user; generating a public key using the non-activated smart card; sending the public key to the administration server; and receiving a digital certificate that is generated using the public key, wherein the non-activated smart card is activated upon receipt of the digital certificate" as recited in independent Claim 9. Claims 10-13 are dependent on Claim 9.

Therefore, Applicants respectfully submit that the Examiner's basis for rejecting Claims 1 and 9 under 35 U.S.C. § 102(b) is traversed and that

these claims are in condition for allowance. Applicants also respectfully submit that the Examiner's basis for rejecting Claims 2-6 and Claims 10-13 under 35 U.S.C. § 102(b) is traversed, as these claims are dependent on allowable base claims and recite additional limitations.

103 Rejections

Claims 7-8, 14-16 and 23-25 are rejected under 35 U.S.C § 103(a) as being unpatentable over Muftic in view of Boroditsky et al. ("Boroditsky;" US 6,332,192). The Applicants have reviewed these references and respectfully assert that the present invention as recited in Claims 7-8, 14-16 and 23-25 is not anticipated nor rendered obvious by Muftic and Boroditsky, alone or in combination.

As presented above, the Applicants respectfully submit that Muftic does not show or suggest the present invention as recited in independent Claims 1 and 9. Claims 7-8 are dependent on Claim 1 and recite additional limitations, and Claims 14-16 are dependent on Claim 9 and recite additional limitations.

Using similar reasoning as that presented above, Applicants respectfully submit that Muftic does not show or suggest the present invention as recited in independent Claim 23. Moreover, Claim 23 clearly distinguishes between a first use of a (non-activated) smart card and subsequent uses of an (activated) smart card.

Specifically, Applicants respectfully submit that Muftic does not

show or suggest "on first use of a non-activated smart card by a user to whom the non-activated smart card has been issued: receiving identifying information for the non-activated smart card; receiving manual identification information for the user; authenticating the user and the non-activated smart card using the manual authentication information and the identifying information; obtaining a public key from the non-activated smart card; and sending a digital certificate generated using the public key from a certificate authority to the non-activated smart card, wherein the non-activated smart card is activated upon receiving the digital certificate" as recited in Claim 23. Claims 24-25 are dependent on Claim 23.

Boroditsky does not overcome the shortcomings of Muftic. Specifically, Boroditsky, alone or in combination with Muftic, does not show or suggest "receiving identifying information for a non-activated smart card that is being used for the first time by a user; receiving manual authentication information for the user to whom the non-activated smart card has been issued; authenticating the user and the non-activated smart card using the identifying information and the manual authentication information; obtaining a public key from the non-activated smart card; and issuing a digital certificate that is generated using the public key, wherein the non-activated smart cart is activated upon receiving the digital certificate" as recited in Claim 1.

In addition, Boroditsky, alone or in combination with Muftic, does not show or suggest "sending, to an administration server, identifying information read from a non-activated smart card that has not been

previously used by a user to whom the non-activated smart card has been issued; sending, to the administration server, manual authentication information input by ~~a~~ the user; generating a public key using the non-activated smart card; sending the public key to the administration server; and receiving a digital certificate that is generated using the public key, wherein the non-activated smart card is activated upon receipt of the digital certificate" as recited in Claim 9.

Also, Boroditsky, alone or in combination with Muftic, does not show or suggest "on first use of a non-activated smart card by a user to whom the non-activated smart card has been issued: receiving identifying information for the non-activated smart card; receiving manual identification information for the user; authenticating the user and the non-activated smart card using the manual authentication information and the identifying information; obtaining a public key from the non-activated smart card; and sending a digital certificate generated using the public key from a certificate authority to the non-activated smart card, wherein the non-activated smart card is activated upon receiving the digital certificate" as recited in Claim 23.

In summary, Applicants respectfully submit that Muftic and Boroditsky, alone or in combination, do not show or suggest the present invention as recited in independent Claims 1, 9 and 23. As such, Applicants also respectfully submit that Claims 7-8 (dependent on Claim 1), Claims 14-16 (dependent on Claim 9), and Claims 24-25 (dependent on Claim 23) are not shown or suggested by Muftic and Boroditsky, alone or in

combination, as these claims are dependent on allowable base claims and recite additional limitations. Therefore, Applicants respectfully submit that the Examiner's basis for rejecting Claims 6-8, 14-16 and 24-25 under 35 U.S.C. § 103(a) is traversed.

CONCLUSION

Based on the remarks and amendments presented above, Applicants request allowance of the present Application.

Based on the arguments presented above, Applicants respectfully assert that Claims 1-16 and 23-25 overcome the rejections of record and, therefore, Applicants respectfully solicit allowance of these Claims.

The Examiner is invited to contact Applicants' undersigned representative if the Examiner believes such action would expedite resolution of the present Application.

Respectfully submitted,
WAGNER, MURABITO & HAO LLP

Date: 10/8/03

William A. Zarbis
Reg. No. 46,120

Two North Market Street
Third Floor
San Jose, California 95113
(408) 938-9060